Number 1-96

security awareness bulletin

Inside

New World of Change

Department of Defense Security Institute, Richmond, Virginia

security awareness bulletin

Approved for open publication — Unlimited reproduction authorized
May 1996

Director
Department of Defense Security Institute
R. Everett Gravelle

Editor
Lynn Fischer

The Security Awareness Bulletin is produced by the Department of Defense Security Institute, Richmond, Virginia. Primary distribution is to DoD components and Federal contractors cleared for classified access under the National Industrial Security Program and special access programs. Our purpose is to promote security awareness and compliance with security procedures through dissemination of information to security trainers regarding current security and counterintelligence developments, training aids, and education methods.

For new distribution or address changes:

Government agencies: DoD Security Institute, Attn: SEAT, 8000 Jefferson Davis Hwy, Richmond, VA 23297-5091, POC Del Carrell, (804) 279-5314/4223, DSN 695-5314/4223; fax (804) 279-6406, DSN 695-6406.

DIS activities: HQ DIS/V0951, 1340 Braddock Place, Alexandria, VA 22314-1651.

DoD contractors: Automatic distribution to each cleared facility. Send change of address to your DIS field office.

Erratum: The following sub-heading and text were omitted from the beginning of page 11 of the last Security Awareness Bulletin 2-95, "The Threat to U.S. Technology." We regret the error.

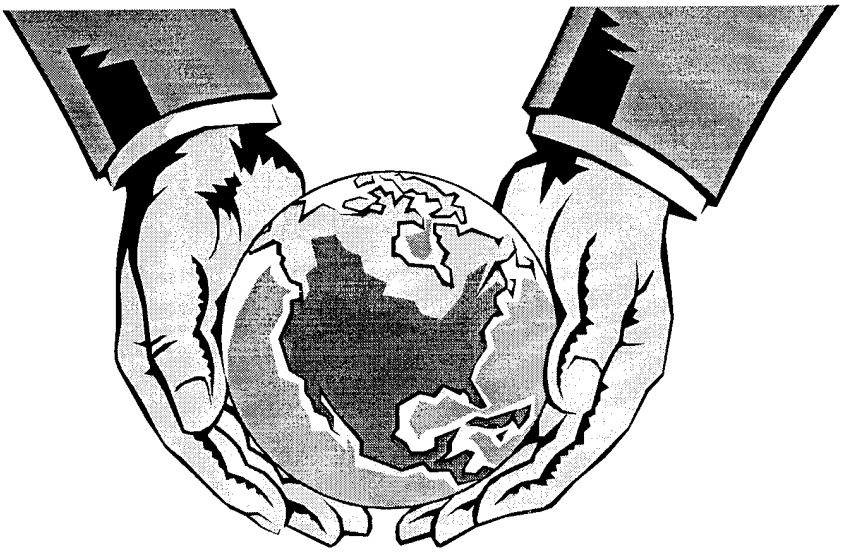
Buyer's naiveté regarding the arms trade

This was a 1988-89 attempt to acquire and illegally export to Iran a large amount of the deadly nerve gas, Sarin. One of the defendants, a U.S.

A New World of Change for Security

The central focus of this issue is the changing environment in which we operate which will require additional education for our employee population. This includes regulatory change, beginning with the new executive orders, and new treaties such as START and the Chemical Weapons Convention (that means that we must prepare ourselves and our employees for something that a decade ago would have been unthinkable: inspections of sensitive facilities by teams of Russian officers). Also in this issue we have included a helpful personnel security job aid on the use of new Standard Forms 85 and 86 which have replaced the older DD Form 398.

This is not the first, nor will it be the last, *Bulletin* which focuses on our changing programs. In July 1995, we distributed a special issue on the National Industrial Security Program to the government contractor community. That issue, which identified the key changes from the older Industrial Security Manual to the new National Industrial Security Program Manual (NISPOM), is available on request to government addressees. In a future *Bulletin* we will focus on the forthcoming Department of Defense regulations covering the personnel security and the information security programs.



The present issue of the *Bulletin*, however, turns the spotlight on the foundation documents for security programs in both government and industry: the new executive orders 12958 and 12968, both promulgated in 1995, which establish the standards, underlying philosophy, and principal guidelines for information security and personnel security regulations across the federal government. We could not hope to cover all aspects of those orders here, but have confined this discussion to those topics and essential changes which security educators need to be conversant with in order to provide preparatory training and initial briefings to their personnel who have been entrusted with the responsibility for protecting national security information.

A New Look at Government Secrecy

The Commission on Protecting and Reducing Government Secrecy

by Eric R. Biel, Staff Director and
Jacques A. Rondeau, Deputy Staff Director

The Commission on Protecting and Reducing Government Secrecy is in the investigative stage of a two-year examination of the federal government's classification, declassification, personnel security, and information security policies. The bipartisan, twelve-member Commission, established by Congress in 1994, is chaired by Senator Daniel Patrick Moynihan (D-NY), and Congressman Larry Combest (R-TX) is its Vice Chairman. Its governing statute calls for "comprehensive proposals for reform" designed to "reduce the volume of information classified and thereby to strengthen the protection of legitimately classified information."

Over the past several months, the Commission has met with officials from a wide range of government agencies involved in either the production or use of classified information. The Commission is also seeking the input of security professionals, government contractors, and all other interested individuals who have thoughts on how best to protect classified and other sensitive government information and to reduce the amount of such information. In early 1997 the Commission will issue a final report outlining recommendations in each of the areas listed above.

The Commission staff includes personnel detailed from the Department of State, the Department of Defense, the National Security Agency, and the Central Intelligence Agency. Several staff members will be focusing in the coming months on coordinating with industry and other private sector organizations that are affected by government classification and personnel security policies. Among the broad issues being addressed by this Commission are the following:

- What government information warrants protection?
- Can certain government information be protected in ways other than classification?
- Does the manner in which industry protects its proprietary information hold any lessons for government?
- What are the costs of classification, declassification, and personnel security systems?
- Are there structural reforms that can enhance the efficiency of classification and personnel security systems?
- What is the "public interest" in protecting and obtaining information?
- How will evolving technologies affect the way information is protected and access is provided?

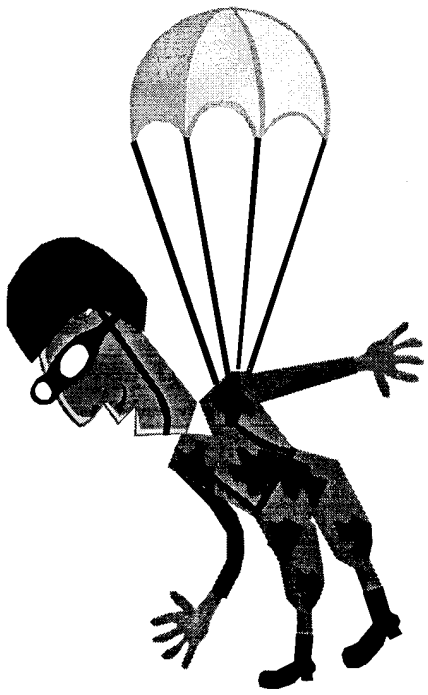
Those interested in contributing their thoughts on these and other issues should contact senior professional staff member John Hancock, coordinator for industry, at (202) 776-8738, or general counsel Sheryl Walter, coordinator for other private sector organizations, at (202) 776-8782. Those who wish to learn more about the Commission may call (202) 776-8725 or email the Commission at ***seccom@ix.netcom.com***.

The Commission on Protecting and Reducing Government Secrecy

Senator Daniel Patrick Moynihan, Chairman
Congressman Larry Combest, Vice Chairman
The Honorable John M. Deutch
Mr. Martin C. Faga
Ms. Alison B. Fortier
The Honorable Richard K. Fox, Jr.
Congressman Lee H. Hamilton
Senator Jesse Helms
Ms. Ellen Hume
Professor Samuel P. Huntington
Mr. John D. Podesta
Mr. Maurice Sonnenberg

Arms Control Inspections:

Are you ready?



Introduction

The United States has signed a host of arms control agreements that will impact facilities far beyond military installations. A few of the more complex agreements are the Strategic Arms Reduction Treaty, Chemical Weapons Convention, and the Open Skies Treaty. Each of these agreements contains provisions to gain unprecedented access to locations and facilities so that professional arms control inspectors may verify specific information. This means that traditional multi-layered risk avoidance measures will not protect classified or sensitive information at affected facilities.

Treaty overviews

The Strategic Arms Reduction Treaty (START)

The only START treaty verification activity that could impact commercial facilities is the "special right of access visit" or SAV. It is in addition to twelve types of START treaty inspections that began following treaty implementation on December 5, 1994. The purpose of the START treaty is to reduce the strategic nuclear forces of the United States and the former Soviet Union. The purpose of a SAV is to assure that nations do not transfer treaty-regulated activities to sites not specified in the treaty. To preclude such an occurrence, the treaty partners agreed to a provision that could lead to an inspection of any facility – government, military, or commercial – suspected of engaging in prohibited activities. Most susceptible are those companies that produce, test, assemble, or maintain components of ballistic missile systems. The treaty does not clearly define how or when a foreign nation may conduct a SAV. It stipulates that the parties concerned will discuss and possibly resolve the issue at an international forum but affords the option of permitting a SAV to alleviate the concern.

Chemical Weapons Convention (CWC)

The CWC is an extremely comprehensive agreement that, when implemented, will directly affect more than 6,000 U.S. facilities. The CWC is designed to eliminate an entire class of weapons of mass destruction. The CWC will require all companies that produce, process, transfer, or consume a wide range of specified chemicals to declare this information, through the U.S. Government, to an international body known as the Organization for the Prohibition of Chemical Weapons (OPCW). The OPCW will send teams of international inspectors to verify the accuracy of the declared information and make reports to the OPCW. Additionally, if any CWC member nation suspects that a prohibited activity is occurring at a facility under U.S. territorial control, it may request a Challenge Inspection. A Challenge Inspection can occur at any site – government, military, commercial, or private – suspected of engaging in prohibited activities. A Challenge Inspection could be remarkably intrusive and begin within days after

arrival of the inspection team in the United States.

The Opens Skies Treaty

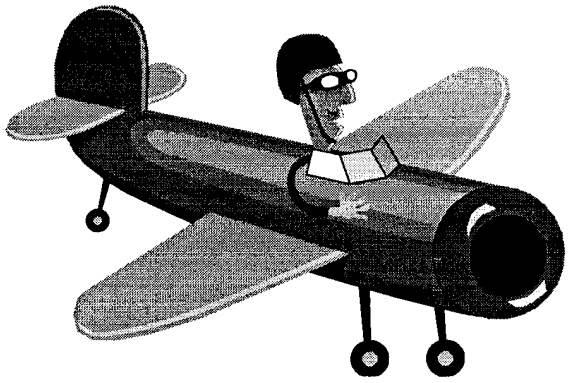
The Open Skies Treaty will impact thousands of U.S. facilities and may be implemented this year. This agreement allows for unimpeded aerial observation of all U.S. territory. Foreign nations may use aircraft equipped with monitoring devices such as optical panoramic and framing cameras, video cameras, synthetic aperture radar, and infra-red line-scanning devices to acquire imagery of any site on U.S. territory. The foreign nation may analyze the imagery themselves or, when requested, sell the film to another treaty partner at nominal cost. Outdoor test and evaluation centers are the most vulnerable to loss of information during Open Skies observation missions. However, even covered facilities could lose information, particularly to the infra-red line scanning device.

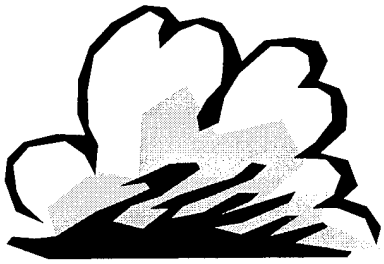
Arms control inspections: Unlike any other

Arms control inspections are unlike any other facility event. During the inspection process, facility managers must grant inspectors access to sufficient areas, records, samples, and information to alleviate their treaty compliance concern. In the process, inspectors may bypass security barriers and request access to rooms, buildings, laboratories, assembly lines, or any other area they suspect is being used for purposes prohibited by the treaty. Although many companies have security programs, most do not address threats posed by the high degree of openness and access granted by law in today's arms control environment.

Are you vulnerable?

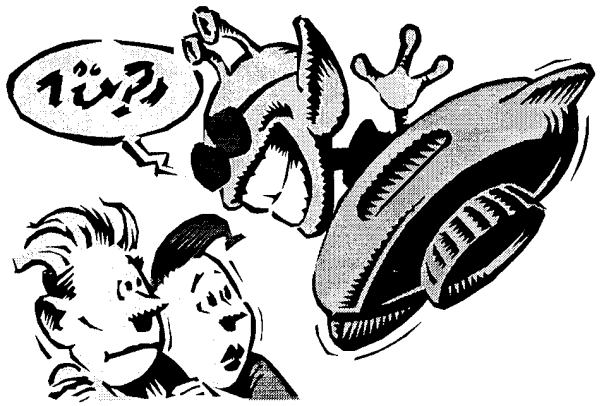
In the emerging arms control environment there is a growing probability that a foreign inspection team will visit private or commercial industries. Foreign inspectors will eventually visit the facilities that report use or storage of chemicals prescribed by the CWC. Likewise, there are a few commercial facilities already subject to START inspections. These facilities have the advantage of time to prepare plans and rehearse inspection procedures. However, thousands more U.S. industries are unaware of their vulnerability to arms control inspections. If you are among the latter group, the challenge is to evaluate your susceptibility and take prudent action. If you do not know your treaty rights and you fail to take precautions, there is a high probability that you will inadvertently disclose sensitive information during an overflight or during a short-notice challenge inspection by foreign nationals.





This article was submitted by the On-Site Inspection Agency.

Foreign Inspectors — At my Facility?



Mike hung up the phone and rushed over to his Security Manager's office. "Larry, I just got a call from the Pentagon...and so did our CEO," he said. "In less than 60 days, a bunch of Russian inspectors want to come here to do something called a special access visit." As the facility's Security Manager, Larry told Mike, "There's no way we can simply allow a team of foreign inspectors to walk through our site – especially with our sensitive R&D operations." The senior Defense official had promised Mike he would send some kind of team to help them, but it wasn't clear to Mike or Larry what kind of "help" was on its way – or what, if anything, they would have to do.

A conversation like Mike and Larry's could take place at your facility in the near future. Under a new arms control agreement called START (Strategic Arms Reduction Treaty) any U.S. facility may be subject to a "visit with special right of access" or SAV in order to satisfy a concern about U.S. compliance with the treaty.

This article has been prepared by the On-Site Inspection Agency (OSIA) for defense contractor site and facility managers, facility security officers, and other senior company officials. It is intended to increase awareness of arms control agreements that can affect facilities anywhere in the United States. The following fictional account introduces the U.S. Government players, and explains the procedures the Defense Department established to assist vulnerable sites and facilities like yours in the event of a START special access visit – because information can be a powerful security countermeasure.

A new era in security

START's entry-into-force (EIF) in December, 1994, marks an important step toward international security in the nuclear age. It also represents the beginning of a series of arms control agreements whose verification provisions permit intrusive inspections of defense contractors and other private U.S. facilities.

The treaty places limits on strategic offensive weapons including ballistic missiles and heavy bombers as well as the nuclear warheads associated with weapon systems. Originally signed with the Soviet Union in 1991, the breakup of that country resulted in a five-party treaty including the United States, the Russian Federation, Ukraine, Kazakhstan and Belarus.

To ensure that all parties observe their treaty commitments, there are a dozen different types of inspections at declared missile or bomber-related facilities, as well as continuous monitoring of mobile ICBM production sites.

Unexpected guests?

What Mike and Larry didn't know is that START also permits treaty parties to request special access visits at any facility – declared or not – including those with no apparent connection to strategic weapon systems controlled by START.

Mike's tone became more sober as he looked at Larry and asked, "We don't make nuclear bombs or missiles, Larry! Why are Russian inspectors allowed to come here..., and what's the purpose of this visit?" He paused, then asked, "What kind of help is the Government offering? We handle foreign visitors all the time, why should we need outside help...?"

Mike and Larry, are about to find out that the United States is committed both to fulfilling its obligations under START, and to demonstrating its compliance whenever necessary. Also, as the site and security managers, Mike and Larry will remain responsible for protecting any classified, proprietary, or other sensitive information under their control from disclosure during all treaty activities– including on-site inspection by foreign inspectors.

Special Access Visits

Each request for a special access visit (SAV) must be based upon an urgent concern about treaty compliance. However, the United States is under no obligation to grant the request. The United States *is* required to attend a special session of the Joint Compliance and Inspection Commission (JCIC) – the treaty's official forum for discussing resolution of compliance concerns – in Geneva, Switzerland.

In order to avoid an intrusive inspection at highly sensitive facilities, U.S. negotiators may try to resolve the compliance concern without granting a SAV. Whether a SAV occurs or not, the U.S. goal is to demonstrate full compliance with the treaty to the satisfaction of all involved parties.

Because a SAV may provide access to normally restricted areas, it increases the opportunity for disclosure of national security, company proprietary, or other sensitive information. Recognizing this concern, the Department of Defense (DoD) developed procedures to assist defense contractors to prepare for START inspections.

Compliance Review Group

Mike recalled the senior Defense official telling him that, "The DoD CRG has been convened to assess the situation and someone will be contacting your facility again for additional information...." The official also emphasized that "...close coordination is necessary during site assessment to ensure both national security and company proprietary interests can be protected." But Mike didn't know what or who the CRG was, nor what was meant by site assessment.

Shortly after the United States is notified of a compliance concern, the DoD START Compliance Review Group (CRG) convenes in Washington, D.C. to develop DoD's recommended response to the compliance concern. The CRG is comprised of senior Defense officials representing acquisition and technology, policy, legal, security, and counterintelligence interests, as well as officials from the Joint Chiefs of Staff. When appropriate, representatives from the military services and On-Site Inspection Agency are also included.

The Compliance Review Group's recommendation goes through the Secretary of Defense to the President's National Security Council staff, which then provides guidance to U.S. representatives at the special JCIC session.

If the concern includes a request for a special access visit, the Defense Department will notify the site or facility manager within hours of receiving the request. The Compliance Review Group needs to quickly evaluate possible alternatives to a SAV, as well as the risks associated with granting a special access visit at the requested facility.

Larry's thoughts drifted back to the company meeting last week where the Division was spotlighted for its cutting-edge research support to the XB-6 program. "Could this SAV expose the program to a foreign intelligence threat?" he wondered aloud. Mike then came to the note he had scribbled during that surprise telephone call. It indicated that a DoD Site Assessment Team would arrive at his site in less than 24 hours. He turned to Larry, "Find out what this team plans on doing and what it needs from us."

Mike and his CEO were unaware of the Department of Defense's procedures for responding to a START compliance concern. So, when the senior Defense official – the Compliance Review Group's representative – at the Pentagon called, they did not realize how the DoD could help them. The CRG begins what it calls the site assessment phase when the facility of concern is identified. This phase is critical in determining not only what will happen in future phases, but whether the United States will grant the special access visit request in the first place.

Assessing Facility Risk

One resource the Compliance Review Group uses to assess the impact of a potential SAV is the DoD Site Assessment Team, or SAT. The SAT can be dispatched rapidly to the affected site, and is comprised of representatives from DoD's Under Secretary of Defense for Acquisition and Technology, Under Secretary of Defense for Policy, Assistant Secretary of Defense for Command, Control, Communications and Intelligence, the military services, and On-Site Inspection Agency.

These personnel work with the facility to develop alternative, less intrusive means of resolving the compliance concern. The SAT also works closely with the site's facility, program, and security managers to identify possible disclosure risks relating to classified, proprietary, or other sensitive information at the site. Indeed, no one knows about sensitive programs and company proprietary interests better than the facility's managers. Finally, the SAT also helps decide how and when the requested special access visit could take place with the least impact to the facility – or whether the SAV should be granted at all.

Because DoD's Site Assessment Team cannot do its job properly without the cooperation of facility personnel, Mike and Larry must also put together a facility response team. The person in charge of this team should have a working knowledge of the facility's operations and site layout.

The team manager's job is to coordinate all site preparatory tasks. Normally, the team manager delegates some responsibilities to functional area managers such as contracts, finance, safety, security, production, scheduling and programs, and emergency services. With so many areas of expertise resident in the company, the facility response team contributes crucial knowledge about all areas that can be affected by a SAV.

After consulting with site management, the Site Assessment Team reports its findings to the Compliance Review Group, which makes its recommendation to the Secretary of Defense. The company's CEO and site manager will be informed as soon as possible of the U.S. Government's decision on how the SAV request will be handled.

If the decision is to allow the SAV, all aspects of the visit—where inspectors can go, what they can do, when they will arrive—are negotiated in the special JCIC session. (Unlike most other arms control agreements, SAV inspection procedures and scope are not predetermined by the treaty.) The JCIC session may last up to 30 days, and the actual date for the SAV will be after that. Consequently, the site could have 1 ½ to 2 months to prepare for the SAV, if it begins when notified by the Compliance Review Group.

After the site assessment phase, Mike was informed that the Government had agreed to the SAV at his site. Larry learned of this decision quickly and said to Mike, "I understand our SAV vulnerabilities now, thanks to what we learned during site assessment. What I need is help developing countermeasures that will protect our rights and still show the Russians that we're not doing anything wrong." "Glad you feel that way," replied Mike, "I was just informed that another DoD group—a Site Preparation Team —would like us to set a date to begin just that kind of thing."

Preparing your site

When the United States grants a SAV request, the Department of Defense sends a Site Preparation Team (SPT) to help managers prepare for the presence of foreign inspectors at their facility. The composition of the SPT is similar to the Site Assessment Team; however, its role is to help the site prepare for the inspection. It can assist any functional area of the facility to prepare for the inspection team's arrival and visit. The SPT also helps facility managers to develop and implement appropriate, cost-effective security countermeasures to protect vulnerable information from disclosure during the inspection.

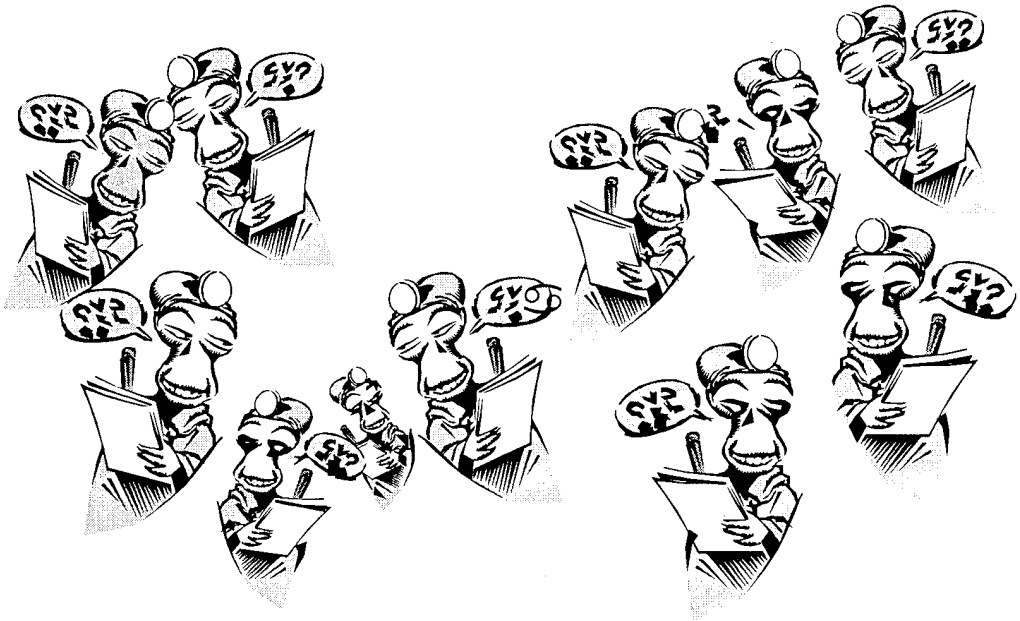
After preparation of the site, the Site Preparation Team may also recommend to the START Compliance Review Group that a mock inspection exercise be carried out. Although not always employed, mock inspections are a good way to validate the security countermeasures developed during site preparation *before* foreign inspectors arrive. Finally, the Site Preparation Team also provides assistance during the actual SAV.

Compliance without compromise

START's entry-into-force brings with it potentially intrusive special access visits – a level of verification unprecedented in arms control history. However, by working with the U.S. Government during site assessment and preparation, facility managers can ensure that the SAV will demonstrate compliance with START without putting national security, proprietary, or other sensitive information at risk.

Moreover, careful coordination with the Government during the site assessment and preparation phases will help keep cost and disruptions of facility operations to a minimum. Finally, proper planning may even contribute to a U.S. decision not to grant a special access visit at all (if the site has identified sufficient alternative means to demonstrate U.S. treaty compliance).

Facility managers, program managers, and especially facility security officers in the defense industry should learn about emerging arms control agreements. In addition to START, the Treaty on Open Skies and Chemical Weapons Convention offer two other agreements that will present different challenges to traditional security measures at sites and facilities across the United States.



For more information on START special access visits, contact the Office of the Under Secretary of Defense (Acquisition & Technology), Arms Control and Compliance at (703) 695-7840. Information on arms control security countermeasures is available by calling the On-Site Inspection Agency's Security Office at 1-800-419-2899 or by contacting your local Defense Investigative Service representative.

Postscript

In the end, Mike and Larry had nothing to worry about. The special access visit conducted by 11 Russian inspectors went smoothly thanks to careful planning and close coordination with the Department of Defense, as well as the site's prior experience hosting foreign visitors. The experience, however, has caused them and their CEO to ask lots of questions about other new arms control agreements that may affect them—like the Chemical Weapons Convention and Treaty on Open Skies.

This article was submitted by the On-Site Inspection Agency.

What you need to know about the new Executive Orders

by Lynn F. Fischer, DoD Security Institute

The long-awaited Executive Orders 12958, Classified National Security Information, and 12968, Access to Classified Information, establish the minimum requirements as well as the underlying philosophy for information and personnel security programs throughout the Federal government. These two foundation documents issued in 1995 are the basis for new and revised regulations on information and personnel security for the Department of Defense, the military departments, defense contractors, as well as other government agencies.

There is much in these executive orders for the security professional to note and inwardly digest. We now have new guidance related to classification management, safeguarding, marking of materials, access to classified information, and individual responsibilities in general. Many things have not changed – for example, the three levels of classification. Something else that has not changed is the requirement to sign a non-disclosure agreement upon being granted a clearance. However, there are some important innovations that will govern the way we gain access to and safeguard classified information. These will be the focus of this article which security educators may wish to use as a guide for briefing their employee populations.

How much do we need to know about the new EOs?

What each employee and service member needs to know about these new orders has a lot to do with the specific professional role he or she plays. Obviously, the security program manager whose organization deals with a significant volume of varied information must keep abreast of all new regulatory changes in detail. But this is not the case for all personnel or even the larger population of cleared employees.

New Marching Orders

With the issuance of these new orders, the security educator or briefing official should be able to convey to their audiences the central features and important changes that might impact on their professional lives regardless of their individual roles. And this includes core information that we, who are routinely responsible for safeguarding materials, should be learning right now through our continuing awareness educational programs.

Security educators: The ball is now in our court

As always, the security educator has the special function of translating the somewhat formal lan-

guage of the regulations and directives, when they appear, into readily understood straight talk for the rank-and-file employee. At this time we are being asked to prepare our people for the changes ahead, in simple but accurate terms, and why these improvements are important. And there is a degree of urgency. For one thing, these executive orders are already in effect and wherever possible, implementation is proceeding throughout the federal government. In addition, new Department of Defense regulations are nearing completion. The point is that our security professionals and cleared personnel need to be prepared for the definitive departmental or agency regulations in a way that will ensure their immediate effectiveness and wholehearted support.

Guidance for security education beyond the Executive Orders

Each order calls for implementing directives that will provide procedural information – in other words, what steps to take to carry out the Chief Executive's intent.

EO 12968: Regarding *Access to Classified Information*, we will be looking to the National Security Policy Board[1] for guidelines for implementing certain provisions such as financial disclosure and investigative standards. At this time, however, we do not have additional new guidance about security education related to EO 12968. But the language of the order itself is fairly specific about what the security educator should do, and these points will be reviewed in this article.

Change 3 to DoD 5200.2-R, *Defense Personnel Security Program*, has recently been released to help bring us in line with the new executive order. Guidance for security awareness and education in Chapter 9 of that regulation has not been altered; however, a full revision of the regulation will be issued later this year and a forthcoming issue of the *Security Awareness Bulletin* will focus on the new regulatory basis for Department of Defense security programs.

EO 12958: *Classified National Security Information.* The Information Security Oversight Office (ISOO) was tasked with developing implementing directives. We have reprinted, as an appendix to this article, the portion of the directive that deals with *Security Education and Training* (subpart D) since it provides clear guidance about the content of different types of briefings and educational communications to our employee populations. ISOO is also responsible for ensuring that federal agencies comply with the directive.

A revised DoD 5200.1-R, *Defense Information Security Program*, is now under review. It will provide updated standards for the security educator in Defense components. Its issuance may in fact coincide with the publication of this issue of the *Bulletin.*

[1] The Security Policy Board is an interagency group that holds responsibility for coordinating security policies across Federal agencies.

Access to Classified Information
Executive Order 12968

Briefing New Employees: What do you tell them up front?

New employees may be individuals who are new to the organization or those who are applying for eligibility for access to classified information for the first time. When they are granted a clearance, their all-important initial indoctrination is a ready-made opportunity for you to discuss with them the essential information contained in the new executive order. This would include principal points about the eligibility standards on which a decision about personnel security clearance is or will be based. In the past we all knew that there was a lot of misinformation floating around about the clearance process. Here is a chance to set the employee's mind at rest and to dispel misconceptions about the clearance process as being some sort of arbitrary or mindless machine.

In brief, the new executive order establishes clear and (for the first time) government-wide eligibility standards and security concerns as well as due process procedures for government employees and service members. On the other side of the coin, it spells out employee responsibilities and obligations, particularly in regard to foreign travel reporting and financial disclosure.

Eligibility standards:

Several important principles are stressed in EO 12968. And these in large part reinforce established policy that has been in effect in the Department of Defense and many other federal departments and agencies. But now these standards are to apply to all of government.

One is that to be eligible for access to classified information, an individual must have a real need for that information to carry out his or her official duties—other justifications are not valid, such as rank or grade or need to get access to controlled areas for convenience sake.

Secondly, the applicant (who must be a U.S. citizen) must be evaluated based on past history or behavior. Here is one way to introduce this idea: If the government is going to place extremely valuable national security information in the care of an employee, we must know beforehand that the employee is reliable. Is that person trustworthy, loyal to the nation, honest, and willing to do those things that would prevent critical information from falling into the hands of persons or interests who would use it against us?

However, there are a couple of new guidelines which have received a lot of notice in the press. One of them is that no agency may discriminate against an applicant for a security clearance solely on the basis of that person's sexual orientation and another is that past mental health counseling is not to be considered as a disqualifying factor.

Actually this has been the general policy in the Department of Defense for many years, although it got scant notice in the public media. The Defense Investigative Service and those who finally make a judgment based on the facts, have followed the principle that any decision about eligibility should be based on a comprehensive picture of an applicant's life and character, including, personal development over time, ethics, vulnerability to being

compromised, and stability. This is known as the "whole person" concept.

Financial disclosure and foreign travel reporting:

Part of that "whole person" that the government needs to see in order to make a fair determination is the applicant's pattern of behavior related to personal finances. Personal financial data could have a negative or positive effect on the final decision. On one hand, a history of financial responsibility is obviously a good indicator of reliability and a sense of responsibility in other areas of life. However, on the other side, excessive indebtedness is known to have made individuals vulnerable to compromise and betrayal as in the case of convicted spy Ronald Pelton or Thomas Cavanagh.[2]

Similarly, unexplained affluence, as in the case of Aldrich Ames, is another red flag, particularly after a person is placed in a position of trust. In a few cases, investigative techniques have revealed evidence of illegal activity, other than espionage, resulting in ill-gotten gains. Obviously that is something we don't want to see among our trusted employees. For these reasons access to personal financial information is quite important.

Therefore, the new executive order requires each applicant to give (as a condition to receiving access) written consent permitting access by the investigating agency to his or her financial records, consumer credit reports, and foreign travel history.

A special category of personnel

There is in this executive order a new requirement for financial disclosure and foreign travel reporting for a certain group of personnel who have or have applied for access to classified information. These employees would have a regular need for or access to particularly sensitive categories of information which include the following:

1. The identities of covert U.S. intelligence sources
2. Technical knowledge about intelligence collection systems
3. Codes and cryptographic systems
4. Special access programs
5. Sensitive nuclear weapon design information

Members of this category make up a small percent of the total population of cleared personnel. Many would be located in intelligence organizations. A lot of people, even those having access to Top Secret information, would not fall into this category of "designated" employees and it is important for the educator to assess an employee population in this regard before determining how much emphasis to place on this particular change.

The new financial disclosure requirement for applicants for a clearance is essentially this: Those employees having access to particularly sensitive information must provide a complete financial report (including information for family members) as part of a background investigation (and later, any reinvestigation). Presumably, applicants not belonging to this group will continue to provide financial information as indicated on the standard forms for clearance application.

Temporary access

The flexibility outlined in this executive order to deal with urgent mission requirements should not be overlooked. Sometimes due to special circumstances or compelling national interest, temporary eligibility for access can be granted while an initial investigation is under way. There are some clear ground rules; it must be justified and must be based on minimum investigative standards. Also, once eligible and working in a position of trust, an employee may be granted temporary access to a higher level, but again under clearly defined conditions.

Review and denials of access:

A question frequently asked by new applicants for a security clearance is, "What happens if they

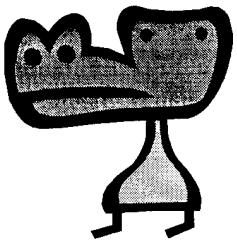
[2] Short summaries of these and other espionage cases can be obtained by ordering *Recent Espionage Cases* from DoDSI. See the ordering form at the back of this issue.

turn it down?" Although the denial rate has consistently been very low – something on the order of 2% of all applicants – this is a fair question that we can now respond to on a more positive note, thanks to the new executive order.

With the implementation of this order, cleared federal employees and military personnel now have a formal appeal process available to them in case of a denial of access to classified information. First of all, in a case of denial (or later revocation, after the initial granting of a clearance) a detailed written explanation will be provided to the applicant. The person may respond in writing, may request a review of the information on which the decision was based, and lastly, will have the opportunity for a formal appeal to a higher-level panel.

Briefing Employees Who Now Have Access:

What's new and different?



Personnel who already have access to classified information also need to know how this EO may affect their professional lives. They can be informed through special briefings, annual refresher briefings, your organization's newsletter, special bulletins, or other methods as appropriate. As with new applicants for access we should advise our experienced personnel about eligibility standards and security concerns. But there is a different approach to other changes for the employees already on-board regarding financial disclosure, foreign travel reporting, and the new due process standards.

For one thing, all employees should be informed about the new review and appeal process where, in extreme cases, access to classified information is revoked. And the provision for government-wide reciprocal acceptance of access eligibility is also something that all currently cleared people should be aware of in this age of governmental right-sizing and shifting of human resources.

Eligibility policy

The eligibility standards discussed earlier also apply to employees already granted access to classified information as they are re-evaluated for continued access under the department or agency's periodic reinvestigation program. Although an individual is eligible for access to information at a level of classification consistent with the employee's requirements for information and no higher, the order does include a provision for temporary access to higher levels. Temporary access cannot exceed 180 days and must be limited to a specific category of information related to an operational requirement that is not expected to occur again.

Annual financial and foreign travel reporting

Part of our responsibility to the cleared employee population is to inform them about new, annual reporting requirements resulting from the executive order. Personnel designated by their agency head as having a regular need for access to particularly sensitive information (as described earlier) will be required to submit an annual financial disclosure statement. This will be done on a new, standard financial disclosure form. Financial disclosure will also constitute an essential part of each reinvestigation as well – to include information about the employee's spouse and dependent children.

Consistent with guidelines to be developed by the Security Policy Board, employees will also file information about their foreign travel. This of course, is a policy that is already common to many federal agencies including the Department of Defense.

To a considerable extent the thrust of this new order is a reflection of the lessons we learned from the recent Ames case. From the time the case broke in February, 1994, official government reports and public media stories catalogued in shocking detail the unaccounted-for affluence literally flaunted by Ames and his wife – from their half-million dollar home to their expensive Jaguar sports car. It is clear that had counterintelligence components acted on these tell-tale signs at an early stage in the crime, much damage would have been averted. Furthermore, Ames's frequent trips to Mexico City

and European capitals to meet with Soviet and Russian handlers should have been a signal for timely investigative action.

Reciprocal acceptance of access

Championed as one of the great cost-saving achievements of the National Industrial Security Program (NISP), the new executive order extends access reciprocity to the Federal agency structure. As a general rule, eligibility for a level of access in one agency will be accepted by others at the same level. Eligible employees will not have to await the outcome of a new background investigation when they move from one agency to another. The only exception would be a situation in which a receiving agency has previously undiscovered information that indicates that the employee would not satisfy the access eligibility standards. The same principle applies to special access program personnel.

Appeal process in the event of revocation of access

Essentially the same due process provisions which apply to denial of eligibility for access also apply to situations where access is revoked. Revocation of access is a rare occurrence when considering the vast population of government and contractor employees who currently hold a clearance. It is the intent of the framers of this order that, none the less, we should all be aware of our legal rights. The order requires that anyone whose access is revoked can receive a written explanation for the reasons, be represented by counsel, reply in writing and request a review of the decision, and appeal to a higher-level panel appointed by the agency head.

What Everybody Ought to Know About the New Executive Order

Employee responsibilities

Cleared employees also have important obligations under this new order. The list of employee responsibilities in this executive order is short, to the point, and in language that could be used directly in a security briefing or memorandum. Each employee granted eligibility for access to classified information is responsible for:

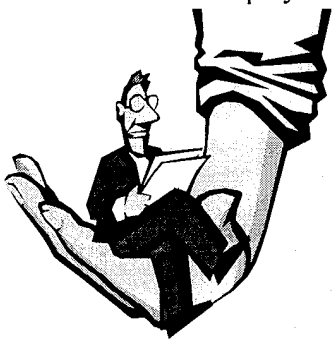
- protecting that information from unauthorized disclosure;
- reporting any attempt by anyone to obtain unauthorized access to it;
- reporting violations of security regulations to security officials;

- complying with all security requirements in this order or implementing regulations; and for
- reporting information "that raises doubts about whether another employee's continued eligibility for access to classified information is clearly consistent with the national security."

Clearly, this last obligation in the context of security education must be carefully presented to our cleared audiences, stressing the positive benefits. A word of advice: Approach the subject of reporting responsibility not from the perspective of mutual suspicion among employees, but from the point of view of concerned co-worker intervention. Official regulations may contain such ominous phrases as "adverse information reporting." But in our role as security educators who are tasked with the job of selling security to sometimes doubting audiences, we should be sensitive about our choice of terms and their impact on motivation. Whenever possible, put a friendly face on employee responsibilities.

A specific mandate for the security educator

The new EO 12968 states that each agency that grants access to classified information shall establish a program to inform and educate those employees about two important things: (1) their individual responsibilities and (2) guidance and assistance available concerning issues that may affect their eligibility for access to classified information, "including sources of assistance for employees who have questions or concerns about financial matters, mental health, or substance abuse."



The significance of the language of point 2 cannot be overstated. While

awareness message with information about employee assistance programs or EAPs. The EAPs currently in place in all Federal agencies offer supervisors and the individual employees an avenue for confronting severe personal problems that might impact on performance and on the safety of everyone in the workplace.

Quite aside from our security interests, employee assistance programs are an effective check against otherwise valuable employees going off the deep end. In case after case of destructive behavior in the workplace, whether it be theft of government property, suicide, violence against other personnel, or even espionage, investigators have documented situations in which troubled employees have acted out of a sense of desperation or a feeling that there is no other way out. The message here is that we should deal with personal problems and crises at an early stage, and certainly before they develop into security problems that might bring into question a person's ability to safeguard valuable information.

This prescription echoes the lessons learned from the *Project Slammer*[3] research reported earlier in the *Security Awareness Bulletin* (2-94): We should certainly be alert and responsive to suspicious activities whether they suggest the compromise or theft of classified information or other types of criminal behavior. But we are more likely to see a much more common occurrence: individuals showing signs of stress or inability to deal with a personal problem. In these instances, the co-worker or supervisor needs to take action in the interest of that person. Involving him or her in an employee assistance program is a good alternative. A report made in confidence to a designated security professional may also be appropriate.

The importance of co-worker and supervisor intervention has also been the subject of recent research on violence in the workplace undertaken by the Defense Personnel Security Research Center (PERSEREC) in Monterey. One of the lessons learned from this recently released study is that effective prevention of workplace violence can be achieved by timely and appropriate response to warning signs.[4]

To reinforce this awareness objective (the importance of proactive behavior by informed employees) in our educational programs, we recommend showing any of the *Countering Espionage* series of videos advertised again in this issue of the *Bulletin.*

[3] Project Slammer is an ongoing research effort within the intelligence community based on in-depth interviews with convicted espionage felons, the family members, and co-workers. The effort is directed toward defining the psychological and motivational basis for espionage.

[4] Combating Workplace Violence, Guidelines for Employers and Law Enforcement," by Howard W. Timm and Callie J. Chandler. This is a PERSEREC research report which is available from the International Association of Chiefs of Police, 515 N. Washington St., Alexandria, VA 22314-2357. The report is also available on the WorldWideWeb at http://www.amdahl.com/ext/iacp/

Don't be confused by the terminology

Determination of eligibility for access (to classified information) is to be based on the criteria established in Executive Order 12968, the standards of DoD 5200.2R,[1] and on a demonstrated or foreseeable need for such access.

Security clearance: In Department of Defense regulations, determination of eligibility for access is referred to as a clearance determination. The issuance or granting (and denial or revocation) of a personnel security clearance is done only by a central adjudication facility following a background investigation and based on adjudicative guidelines for determining eligibility for access to classified information.

Interim security clearance: In some cases, a temporary security clearance (or temporary eligibility for access) can be based on the completion of minimum investigative standards and the meeting of certain administration requirements pending the completion of the full investigative requirements.

Access to classified information: The ability and opportunity to obtain knowledge of classified information. Access is controlled by the activity to which a person is assigned.

To have access to classified information, an employee must possess an appropriate clearance (or must have been determined to be eligible) and have a need to know that information.

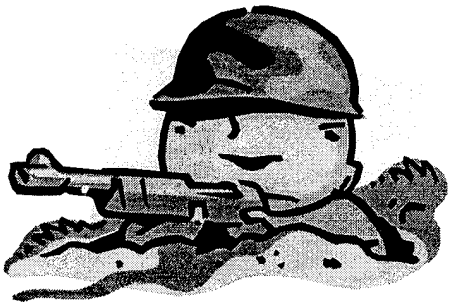
Adjudication: The process of making a decision or judgment about a person's eligibility for access to classified information based on information produced by an investigation and a set of standards or criteria that must be met before a favorable decision can be made. Adjudication is accomplished by a central adjudication facility within the Department of Defense.

Determination of suitability: A personnel decision concerning the hiring or retention of persons for employment by the government. This should not be confused with a security determination.

Suspension of access: An action taken by an activity whereby a person's access to classified information is temporarily suspended pending an investigation and/or favorable adjudication of derogatory information which could affect that person's continued eligibility.

[1] Department of Defense Regulation 5200.2R, *Personnel Security Program*, originally issued in January 1987, has been updated by "Change 3" to reflect the new executive order.

Classified National Security Information Executive Order 12958



We now turn from executive guidelines concerning who should have access to classified information to a focus on the information itself – its control and protection. The new executive order, Classified National Security Information, came into effect on October 14, 1995. As with Executive Order 12968, EO 12958 and its implementing directive (OMB Directive #1, issued by the Information Security Oversight Office), form the basis for agency and departmental regulations across the Federal structure.

As did the executive order it now supersedes[1], EO 12958 prescribes a uniform system for managing the protection of national security information. It describes two classification processes: original classification and derivative classification, and as before, three levels of classification: Top Secret, Secret, and Confidential. And the new order does not significantly change the requirements for safeguarding classified national security information.

The driving forces behind EO 12958

What is new and important are standards that are intended to reduce the enormous inventory of classified materials which have been accumulating since World War II, and secondly, will prevent a further unmanageable volume in years to come. Although there are several important changes resulting from EO 12958, it would appear from the press coverage of this new order that its controversial feature has to do with declassification. Although media reports tended to focus on the number of years that would elapse before automatic declassification kicks in, the fundamental change incorporated in this document is that from now on someone will have to take specific action to stop the declassification of a piece of information (that is, prevent automatic declassification), whereas before, specific action had to be taken to get something declassified.

To help clear the deck of this massive stockpile, which is extremely expensive to maintain, and to make useful information available to our citizens, the President has prescribed an automatic declassification rule of 25 years for most information classified under previous orders as well as this one. From now on, the new standard for declassification is that information will be classified for ten years or less. There are provisions for longer protection but they require specific action on the part of designated officials.

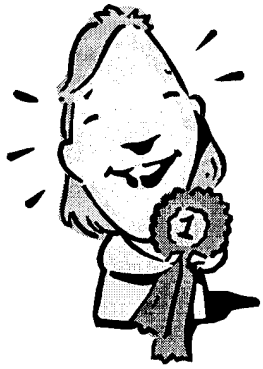
Another important objective of this order is to prevent over-classification of information. Over-classification includes classifying information at too high a level as well as classifying something that shouldn't be classified at all. As this order is implemented, classifiers will have to justify what they classify and, as an additional safeguard, employees will be encouraged and expected to challenge improper classifications. It is with this last type of action – challenges – that all of us ought to be familiar as we routinely work with classified materials.

[1] Executive Order 12356, signed by President Reagan in April 1982.

Enhanced accountability

The order also increases personal accountability for the management of classification and declassification. It details procedures for marking and safeguarding classified materials that exceed previous standards, to include the identification of the classifier and the justification for classification right on the document or material. And it establishes new requirements for classification challenges, self inspection programs, and the oversight of special access programs.

There is one other innovative change that will provide a healthy dose of motivation to those who might otherwise assign a lower priority to security than they should. The order adds classification management as a critical element in performance reviews for certain employees who handle and create classified information. This means that, for some of us, our performance evaluations will be affected by how well we live up our security obligations.



But don't forget the main purpose

We should not overlook the fact, however, that the central purpose of information security programs in government and defense industry is to prevent unauthorized disclosure of valued information. Protecting information vital to our nation's security remains the highest priority.

Specific Changes You Ought to Know About As A Result of EO 12958:

Be prepared to see more detailed document markings

Consider reminding your cleared personnel of the following: While a very few, senior individuals are given the responsibility for original classification, many who routinely work with classified information must be concerned with what is called derivative classification. Examples of derivative classification include writing a report which contains classified information from another source and creating a new document which contains test data or facts which fall into a category of information identified in a classification guide as being classified at a specific level.

So all of us will need to know what document markings mean – not only the standard page, portion, and title markings that indicate the level of classification, but also the information that will appear in the "classification block" on the front of each classified document from now on.

The new classification block strengthens accountability for original classification decisions by including more detailed information than before. The block will indicate the identity of the original classifier, a concise reason for classification, and the date of future declassification which will normally be in ten years unless the information is exempted from the 10-year rule. An exemption can be justified for one of several specific reasons stated in the new EO and the classifier must identify which one, in the classification block. For example, one reason for exemption is that the information reveals an intelligence source, method, or cryptologic system. There are a number of other types of information (listed in the EO) that if revealed publicly even after ten years could do damage to national security.

Derivative classification

The point is that for many of us who are routinely or even occasionally involved in derivative classification, we have to identify the source or sources of the classified information on the new product which we produce. And when we create a new document, video, report, memorandum, photograph, graphic design, or anything that becomes classified through derivative classification, we must add a properly completed classification block to our new item.

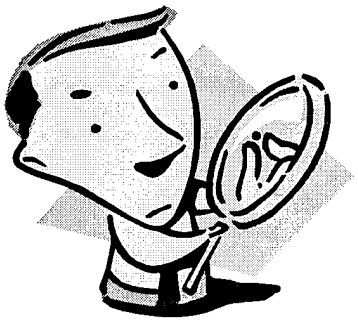
When more than one source is used, the order states that we must mark our new document or material with the highest classification of any of the information we have used and also carry forward to any newly created documents the date or event for declassification that corresponds to the longest period of classification among the sources used. And as mentioned, the new product must carry a listing of all the classified sources from which we have drawn information.

Classification challenges

If we see a document that we think has been improperly classified, what should we do? EO 12958 has established guidelines for formally challenging the classification assigned to information. The order states that those who challenge a classification will be protected from retribution. In fact, we are encouraged and expected to challenge the classification of information if we believe it is improper. Before resorting to the formal challenge procedures, however, an attempt should be made to resolve the matter informally.

The order requires that every formal challenge be reviewed by an impartial official or panel. The Interagency Security Classification Appeals Panel[2] will serve as the final review authority. But each agency will develop specific procedures for challenging a classification and will assign responsibilities for managing the challenge process. Since agencies will also establish procedures for handling appeals, we should expect to hear more on this subject in the near future.

Self-inspection requirements



The order calls for annual self-inspection programs in every agency. Self-inspection is the internal review and evaluation of an agency's program as established by the new order and its implementing directives. Although self-inspections were not prescribed by the previous executive order (EO 12356) or in the current Department of Defense Regulation for our Information Security Program, in practice, many civilian and military organizations regularly use the self-inspection method as a check against serious security vulnerabilities. For others, it may be something new.

Here we can learn something from the National Industrial Security Program in which formal self-inspections at periodic intervals are prescribed by the National Industrial Security Program Manual (NISPOM). A handbook for self-inspections in industry was issued as part of the Security Awareness Bulletin 1-95. Although much in this handbook pertains to government contractors, some of what is offered, particularly concerning employee interviewing, may be helpful on the government side.[3]

Self-inspections should include a review of samples of classified documents that the agency has generated. The primary purpose of these self-inspections is to continually improve the classification process and the information security program, especially helping employees to make better classification decisions.

Security as a critical element in performance reviews

The order adds classification management as a critical element for evaluation during performance reviews for employees (civilian or military personnel) "whose duties significantly involve the creation or handling of classified information." According to the order, this will include those persons authorized to originally classify information, security managers, and security specialists. Beyond this, although exact guidance from the Department of Defense is forthcoming, we can safely assume that it will include persons who are designated as security officers for their organizations on a full-time or part-time basis, or as an additional duty.

---

[2] The Interagency Security Classification Appeals Panel is established by Section 5.4 of EO 12958 and consists of six members who decide on appeals to classification challenges, decide on exemptions from automatic declassification, and decide on appeals to requests for mandatory declassification review.

[3] *Security Awareness Bulletin 1-95* on the National Industrial Security Program was not distributed to most governmental or military security offices. However, a copy may be obtained by using the publications order form that is found at the back of this issue.

A new reality and democratic values

No doubt about it, change seems to be accelerating. We have to deal with new ideas and new working conditions, even a new world order since the collapse of the Soviet Bloc. The recently issued executive orders related to security programs are a part of our government's response to a changing international threat to U.S. critical information and to internal criticisms about the way in which security programs have been managed in the past. What we see here is an effort not only to rectify previous shortcomings, but to ensure uniformity and consistency in policy throughout the federal government. But we also see in both new orders attempts, in the national interest, to mediate among important values.

The new order on Access to Classified Information attempts to strike a balance between the government's need to restrict access to critical information to employees who can be trusted, and on the other hand, the need to ensure that those individuals who are entrusted with the nation's secrets are dealt with fairly and equitably. In keeping with constitutional principles, they are entitled to due process and impartiality under the law, without fear of discrimination.

Underlying the executive order on Classified National Security Information is an attempt to establish another healthy balance between the national interest in protecting vital information on one hand, and on the other, the need for free access to information that should be available to members of the general public. Our democratic principles require that the American people be informed of the activities of their government. And our nation's progress depends on that free flow of information. In recent years, dramatic changes have altered, though not eliminated, the national security threats that we confront. These changes now provide a greater opportunity to emphasize our commitment to open government.

By presenting these new executive orders in the light of these commonly held values and national objectives we reinforce the credibility of our security programs in the eyes of our employee populations and of the general public.

Attention vendors of security software:

The Department of Defense Security Institute invites vendors to send us demo packages and promotional materials related to security products which we would make available to our students here at DoDSI in Richmond. As you know, our student population is generally made up of security professionals, most of whom are new to this field and very interested in the latest products that might help them in their various tasks.

Our plan is to set up a PC in our class room area with all demos provided to us and to display any promotional materials or flyers that students might take away for future reference. It should be understood that the inclusion of materials or software demos for any product does not constitute an endorsement or evaluation by the Institute or the Department of Defense.

Office of Management and Budget, Information Security Oversight Office

Directive No. 1, Classified National Security Information

Subpart D – Security Education and Training

Effective date: October 14, 1995

§2001.40 General [5.6]

(a) *Purpose.* This subpart sets standards for agency security education and training programs. Implementation of these standards should:

(1) Ensure that all executive branch employees who create, process, or handle classified information have a satisfactory knowledge and understanding about classification, safeguarding, and declassification policies and procedures;

(2) Increase uniformity in the conduct of agency security education and training programs; and

(3) Reduce improper classification, safeguarding, and declassification practices.

(b) *Applicability.* These standards are binding on all executive branch departments and agencies that create or handle classified information. Pursuant to Executive Order 12829, the NISPOM prescribes the security requirement, restrictions, and safeguards applicable to industry, including the conduct of contractor security education and training. The standards established in the NISPOM should be consistent with the standards prescribed in Executive Order 12958 and of this part.

(c) *Responsibility.* The senior agency official is responsible for the agency's security education and training program. The senior agency official shall designate agency personnel to assist in carrying out this responsibility.

(d) *Approach.* Security education and training should be tailored to meet the specific needs of the agency's security program, and the specific roles employees are expected to play in that program. The agency official(s) responsible for the program shall determine the means and methods for providing security education and training. Training methods may include briefings, interactive videos, dissemination of instructional materials, and other media and methods. Agencies shall maintain records about the programs it has offered and employee participation in them.

(e) *Frequency.* The frequency of agency security education and training will vary in accordance with the needs of the agency's security classification program. Each agency shall provide some form of refresher security education and training at least annually.

§2001.41 Coverage [5.6(c)(3)].

(a) *General.* Each department or agency shall establish and maintain a formal security education and training program which provides for initial and refresher training, and termination briefings. This subpart establishes security education and training standards for original classifiers, declassification authorities,

security managers, classification management officers, security specialists, and all other personnel whose duties significantly involve the creation or handing of classified information. These standards are not intended to be all-inclusive. The official responsible for the security education and training program may expand or modify the coverage provided in this part according to the agency's program and policy needs.

(b) *Elements of initial coverage.* All cleared agency personnel shall receive initial training on basic security policies, principles and practices. Such training must be provided in conjunction with the granting of a security clearance, and prior to granting access to classified information. The following areas should be considered for inclusion in initial briefings.

(1) *Roles and responsibilities.*

(i) What are the responsibilities of the senior agency official, classification management officers, the security manager and the security specialist?

(ii) What are the responsibilities of agency employees who create or handle classified information?

(iii) Who should be contacted in case of questions or concerns about classification matters?

(2) *Elements of classifying and declassifying information.*

(i) What is classified information and why is it important to protect it?

(ii) What are the levels of classified information and the damage criteria associated with each level?

(iii) What are the prescribed classification markings and why is it important to have classified information fully and properly marked?

(iv) What are the general requirements for declassifying information?

(v) What are the procedures for challenging the classification status of information?

(3) *Elements of safeguarding.*

(i) What are the proper procedures for safeguarding classified information?

(ii) What constitutes an unauthorized disclosure and what are the penalties associated with these disclosures?

(iii) What are the general conditions and restrictions for access to classified information?

(iv) What should an individual do when he or she believes safeguarding standards may have been violated?

[*Editor's note*: The following paragraph (c) of this implementing directive is intended for employees whose duties involve significantly greater responsibility for classified information – such as original classification and other functions typical of security professionals. In paragraph (d) the directive returns to the subject of security education for all cleared personnel.]

(c) *Specialized security education and training.* Original classifiers, authorized declassification authorities, individuals specifically designated as responsible for derivative classification, classification management officers, security managers, security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information should receive more detailed training. This training should be provided before or concurrent with the date the employee assumes any of the positions listed above, but in any event no later than six months from that date. Coverage considerations should include:

(1) *Original classifiers.*

(i) What is the difference between original and derivative classification?

(ii) Who can classify information originally?

(iii) What are the standards that a designated classifier must meet to classify information?

(iv) What is the process for determining duration of classification?

(v) What are the prohibitions and limitations on classifying information?

(vi) What are the basic markings that must appear on classified information?

(vii) What are the general standards and procedures for declassification?

(2) *Declassification authorities other than original classifiers.*

(i) What are the standards, methods, and procedures for declassifying information under Executive Order 12958?

(ii) What are the standards for creating and using agency declassification guides?

(iii) What is contained in the agency's automatic declassification plan?

(iv) What are the agency responsibilities for the establishment and maintenance of a declassification database?

(3) *Individuals specifically designated as responsible for derivative classification, security managers, classification management officers, security specialists, or any other personnel whose duties significantly involve the management and oversight of classified information.*

(i) What are the original and derivative classification processes and the standards applicable to each?

(ii) What are the proper and complete classification markings, as described in subpart B of this part?

(iii) What are the authorities, methods, and processes for downgrading and declassifying information?

(iv) What are the methods for the proper use, storage, reproduction, transmission, dissemination and destruction of classified information?

(v) What are the requirements for creating and updating classification and declassification guides?

(vi) What are the requirements for controlling access to classified information?

(vii) What are the procedures for investigating and reporting instances of security violations, and the penalties associated with such violations?

(viii) What are requirements for creating, maintaining, and terminating special access programs, and the mechanisms for monitoring such programs?

(xi) What are the procedures for the secure use, certification, and accreditation of automated information systems and networks which use, process, store, reproduce, or transmit classified information?

(d) *Refresher security education and training.* Agencies shall provide refresher training to employees who create, process or handle classified information. Refresher training should reinforce the policies, principles and procedures covered in initial and specialized training. Refresher training should also address the threat and the techniques employed by foreign intelligence activities attempting to obtain classified information, and advise personnel of penalties for engaging in espionage activities. Refresher training should also address issues or concerns identified during agency self-inspections. When other methods are impractical, agencies may satisfy the requirement for refresher training by means of audiovisual products or written materials.

(e) *Termination briefings.* Each agency shall ensure that each employee granted access to classified information who leaves the service of the agency receives a termination briefing. Also, each agency employee whose clearance is withdrawn must receive such a briefing. At a minimum, termination briefings must impress upon each employee: The continuing responsibility not to disclose any classified information to which the employee had access and the potential penalties for non-compliance; and the obligation to return to the appropriate agency official all classified documents and materials in the employee's possession.

(f) *Other security education and training.* Agencies are encouraged to develop additional security education and training according to program and policy needs. Such security education and training could include:

(1) practices applicable to U.S. officials traveling overseas;

(2) procedures for protecting classified information processed and stored in automated information systems;

(3) methods for dealing with uncleared personnel who work in proximity to classified information;

(4) responsibilities of personnel serving as couriers of classified information; and

(5) security requirements that govern participation in international programs.

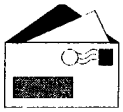
For further information, contact Steven Garfinkel, Director ISOO, telephone (202) 395-7450

Department of Defense
Security Institute

PERSONNEL SECURITY JOB AID

J. Alease Black (ext. 4440)
Ronald W. Morgan (ext. 4364)
Kenneth E. Sudol (ext. 5439)

(804) 279-4440
DSN 695-4440



DoD Security Institute, Building 33E
ATTN: Personnel Security Team
c/o Defense General Supply Center
8000 Jefferson Davis Highway
Richmond, VA. 23297-5091

(804) 279-4527
DSN 695-4527

Use of the Standard Forms 85 P, 85 PS, and 86

Purpose: This job aid is designed to help security personnel prepare requests for personnel security investigations (PSIs). It covers uses of the Standard Forms (SF) 85 P, 85 PS, and 86. These forms are used to collect personal information from people. It does not cover use of the SF 85 for Nonsensitive positions since this form is not used to request PSIs for sensitive duties or classified access. The DD Form 1879, DoD Request for Personnel Security Investigation, has been revised (Sep 95) to be used with the new forms.

Summary of this Job Aid:

- Why are the new forms being used?
- When must the new forms be used?
- Obtaining the Electronic Personnel Security Questionnaire containing the new forms
- Change in the amount of information collected (Time periods have changed.)
- New general and medical releases
- What types of duties or accesses are the forms used for?
- Preparing requests for PSIs using the new forms
- Differences in codes between manual and electronic versions

Point of Contact: Ronald W. Morgan

Why are the new forms being used?

The new SFs are now being used for several reasons:

- The DD forms are expiring.
- The previous versions of the SFs are expiring.
- The Office of Management and Budget has mandated use of the new forms for all Federal agencies.

When must the new forms be used?

- The new SFs may be used beginning 1 Sep 95.
- The new SFs will be the only forms used to collect personal information after 31 Dec 95.
- The DD Forms 398 and 398-2 may be used until 31 Dec 95.
- DD Form 1879, revised Sep 95, must be used after 31 Dec 95.

What are the new forms used for?

- ***SF 86*** is used for all classified access (security clearance, Sensitive Compartmented Information, Special Access Programs) and enlistment/commissioning of military personnel.
- ***SF 85 P*** is used for personnel performing sensitive duties that do not require access to classified information.
- ***SF 85 PS*** is used as a supplemental form to the SF 85 P for designated positions.

Change in the time periods

The SF 85 P and SF 86 ask for *seven years* of information in several items and "have you ever" in others. The DD forms requested either five or ten years of information.

Releases for SFs 85 P and 86

- General release is valid for five years or until affiliation ends.
- Release of medical information is valid for one year or until affiliation ends.

Electronic Personnel Security Questionnaire (EPSQ)

Version 1.2a, Sep 95, contains

- SF 86;
- SF 85 P;
- SF 85 PS;
- DD Form 1879 (revised Sep 95).

How to obtain the EPSQ (for security officers/security managers only)

Call 1-800-755-1520 or FAX the following information to (410) 631-0110 at the Defense Investigative Service (DIS)

- agency name
- full mailing address
- name and title of point of contact
- telephone numbers: regular, DSN, and FAX
- disk size (3.5" or 5.25")
- Contractors – provide your Commercial and Government Entity Code (CAGE).

This version of the EPSQ permits the user to validate the package and

- print out the information to mail to DIS.
- transmit electronically to DIS via CompuServe.
- transmit electronically to DIS via the Internet.

When to Use the Standard Forms 85 P and 86

Duties	Military [1]	Civilian	Contractor	DD 1879	SF 86	SF 85P
Secret and Confidential clearance	NAC or ENTNAC	NACI [2]	NAC		X	
Top Secret clearance	SSBI [3]	SSBI [3]	SSBI [3]	X	X	
Critical-sensitive duties without access	SSBI [1,3]	SSBI [3]	SSBI [3]	X		X
Noncritical-sensitive duties without access	NAC or ENTNAC [1]	NACI [2]	NAC			X
Enlistment, first term	ENTNAC				X	
Commissioning	NAC				X	
SCI	SSBI [3]	SSBI [3]	SSBI [3]	X	X	
SIOP-ESI	SSBI [3]	SSBI [3]	SSBI [3]	X	X	
Special Access Programs - noncritical-Secret	NAC	NACI	NAC		X	
Special Access Programs - critical- Top Secret	SSBI [3]	SSBI [3]	SSBI [3]	X	X	
Secret Reinvestigation	SPR	SPR	SPR		X	
Reinvestigation Critical-sensitive duties with access	PR [3]	PR [3]	PR [3]	X	X	
Reinvestigation Critical-sensitive duties without access	PR [1,3]	PR [3]	PR [3]	X		X
Limited Access Authorization	SSBI [3]	SSBI [3]	SSBI [3]	X	X	
ADP-1, no access	SSBI [1,3]	SSBI [3]	SSBI [3]	X		X
ADP-2 or ADP-3, no access	NAC or ENTNAC [1]	NACI [2]	NAC			X
Critical Nuclear PRP	SSBI [3]	SSBI [3]	SSBI [3]	X	X	
Controlled Nuclear PRP	NAC	NACI	NAC		X	
Chemical PRP	NAC	NACI	NAC		X	
Presidential Support 1 & 2	SSBI [3]	SSBI [3]	SSBI [3]	X	X	
Investigative & Support duties	SSBI [3]	SSBI [3]	SSBI [3]	X	X	
NATO COSMIC	SSBI [3]	SSBI [3]	SSBI [3]	X	X	
NAFI Position of Trust		NAC	NAC			X
Unescorted entry		NAC	NAC			X

[1] Use only SF 86 for all military investigations. [2] Summer hire civilian employees use the NAC. [3] Do not submit supplemental forms for spouse, cohabitant, or foreign born family members checks. Information will be taken from the SFs 85P/86.

PSIs are: SSBI=Single Scope Background Investigation PR=Periodic Reinvestigation SPR=Secret Periodic Reinvestigation NAC-National Agency Check ENTNAC=Entrance NAC NACI=National Agency Check with Written Inquiries

Administrative Information on Standard Forms 85 P and 86

The SFs 85 P and 86, when used for the NAC, ENTNAC, NACI, and Secret PR, require that administrative information be provided on the form itself. This is similar to how administrative information was placed on the old DD Form 398-2. When the DD Form 1879 is used for the SSBI, PR, Expanded NAC, and SII, the administrative information is not placed on the form.

PSIs: Requiring DD Form 1879	PSIs: Administrative Information on Form
SSBI	NAC
PR	ENTNAC
Expanded NAC	NACI
Special Investigative Inquiry (SII)	Secret PR

The following explains how to place administrative information on page 1, items A - P, of the SFs 85 P and 86. The SF 85 PS does not include administrative information as it is included with the SF 85P. The bold print in the left column is what you see on the forms. If there is information in parentheses below the item letter, it indicates the DoD use of the item.

A	**Type of Investigation**	Enter numeric code	**1** NAC - Military **2** NAC - Civilian **3** NAC - Industrial **4** ENTNAC **5** NAC - Other (specify in Block B) **6** Secret Periodic Reinvestigation (SPR)
B	**Extra coverage**		Used to specify type of investigation when "Other" is entered in Block A.
C	**Sensitivity/Risk Level** (Requester Code)		Enter one of the following alpha or numeric codes: **A** Army **F** Air Force **G** Coast Guard **M** Marines **N** Navy **C** Defense Contract Audit Agency (DCAA) **4** Defense Industrial Security Clearance Office (DISCO) **Y** Defense Information Systems Agency (DISA) **I** Defense Intelligence Agency (DIA) **K** Defense Logistics Agency (DLA) **P** Defense Mapping Agency (DMA) **U** Defense Nuclear Agency (DNA) **H** Defense Office of Hearings and Appeals (DOHA) **R** Defense Security Assistance Agency (DSAA) **B** DoD Inspector General (DODIG) **E** General Accounting Office (GAO) **J** Joint Chiefs of Staff (JCS) **L** Library of Congress (LOC) **S** National Security Agency (NSA) **D** Washington Headquarters Services (WHS) **W** White House **O** On Site Inspection Agency (OSIA) **X** Other

D	**Compu/ ADP** (Reason for Request)	You may enter multiple codes if applicable. ***Clearance/Access*** **S** Secret **C** Confidential ***Commission*** **P** Commission (e.g., ROTC, Officer Candidate, Service Academy) ***Enlistment*** **E** Enlistment ***Other Reasons*** **AL** A-12 Litigation **AD** ADP II/ADP III **AA** Area Access **BP** Building Pass - DoD **PS** Building Pass - Press Personnel **CS** Chemical Surety **CA** Circle A2 **RC** Civilian Marksmanship Rifle Club **CM** Civilian Marksmanship M-1 Rifle Purchase **SA** COMSC/T-AGOS Crew Member - Ship Access **CG** Contract Guards **EO** Education/Orientation **FA** Federal Aviation Administration (FAA) **YF** MSM Yankee Fire (no clearance) **MC** Munitions Carriers **NF** NAFI **CC** NAFI/Child Care **NT** NATO **NU** Personnel Reliability Program (PRP) **US** Red Cross/USO **SH** Summer Hire **UE** Unescorted Entry **UI** Unsalaried Interns **YL** Yankee Legacy **XX** Other (specify in Block E)
E	**Nature of Action Code**	Used to specify Reason for Request when "Other" is entered in Block D.
F	**Date of Action** (Date) **Month Day Year**	Leave blank.
G	**Geographic Location** (Organization Code)	Enter the organization code for the organization requesting this investigation. If military, enter the Unit Identification Code (UIC), or Personnel Accounting System (PAS) Code. If contractor, enter the Commercial and Government Entity Code (CAGE) for your facility. If not applicable to the request, leave this block blank.

H	**Position Code** (Status Information)	Enter the code (A through E) for Subject's current status. See below detailed instructions for further data requirements for each status listed. **A** Consultant. Provide contract number for which clearance is required in Block I. **B** Contractor Employee. Provide contract number for which clearance is required in Block I. **C** Key Management Personnel (Formerly identified as Owners, Officers, Directors, and Executive Personnel (OODEP). **D** U.S. Government Employee. For CURRENT government employee, enter grade in Block I. If Subject is an APPLICANT, enter "Applicant," Block I. **E** Military. Enter rank in Block I. If the Subject is an applicant (either enlistee or officer candidate), enter "Applicant" in block I. Following Rank/Applicant entry, enter "N" for National Guard or "R" for Reserve status, if applicable.
I	**Position Title**	To be used in conjunction with Block H.
J	**SON**	Local Files Checked with Favorable Results. Enter "Y" for yes; enter "N" for no. If answer is "N," you must explain in Block O.
K	**Location of Official Personnel Folder** None NPRC At SON	Under "Other Address" enter the following addresses: **Industrial Clearance Requests** Defense Industrial Security Clearance Office P.O. Box 2499 Columbus, OH 43216-5006 **All Other NAC Requests** Defense Investigative Service National Agency Check Division P. O. Box 1083 Baltimore, MD 21203-1083 **Secret PRs** Defense Investigative Service Investigations Division P. O. Box 454 Baltimore, MD 21203-0454
L	**SOI** (Citizenship Verified)	Enter a "Y" for yes; enter an "N" for no. If your answer is "N" you must provide an explanation in Block N.
M	**Location of Security Folder** None At SOI NPI	Under "Other Address" enter the name and mailing address of the organization that the investigation should be sent to upon completion. Note: trustworthiness determinations must be returned to the Government entity sponsoring the investigation and not directly to the contractor or Subject of Investigation. Please ensure that the mailing address is complete, accurate, and legible to include ZIP code.
N	**OPAC ALC Number**	To be used in conjunction with Block L.
O	**Accounting Data and/or Agency Case Number**	To be used in conjunction with Block J.
P	**Requesting Official**	Enter the requesting official's name, title, and phone number in this block. Sign and date the form.

Additional Information on the Manual Forms and the EPSQ

If you prepare both the manual and electronic versions of the forms, there are two differences in the codes used. The differences are noted below.

Manual Version of Forms	EPSQ
Block A, Type of Investigation. There are six codes listed for type of investigation requested. If you are requesting a Secret Periodic Reinvestigation (SPR), type "6."	When you are requesting the type of investigation, it does not give you the option of an SPR. In Module 2, to request an SPR, type "5-Other," press Enter, and go on to the next blocks. When you get to Module 6, the "Reason for Request," you are given three choices. Press the "F6" to get the pull-down menu for reasons. A pop-up screen will ask you to identify the reason for your request. On reason #1, select "S" for Secret clearance. On reason #2, select "XX-Other." The program will then ask you to describe the reason. Type "Secret Periodic Reinvestigation."
Block H, Position Code (DoD uses these codes for the status of the Subject). The codes used are alpha codes: **A.** Consultant **B.** Contractor Employee **C.** Key Management Personnel **D.** U.S. Government Employee **E.** Military	The EPSQ uses numeric codes for the status of the Subject. Module 4 (when completing a NAC) uses these codes: **1.** Contractor Employee **2.** Consultant **3.** Key Management Personnel **4.** U.S. Government Employee **5.** Military

A New CI Video.....

.....from the National Counterintelligence Center

"Something Wasn't Right"

...Highlights how one aware person can make a difference by timely reporting of suspicious behavior.

This 18-minute unclassified video was produced by the NACIC, in conjunction with the FBI, & DOE, and features several significant cases:

- Capture of FALN members in Evanston, Illinois
- Pollard espionage case
- U.S. Customs Service investigation of Dr. Ronald Hoffman

Order from:

Copymaster Video Inc.
P.O. Box 684
Villa Park, IL 60181

Phone (708) 279-1276 or Fax (703) 279-0132

$9.95 (prepaid) includes duplication postage and handling.
(For non-prepaid orders call Copymaster Video.)

Security Program Improvement Network

Calling all bright lights and inventors

Give Security An Electronic Boost

*M*any of you are giving your security programs a real boost in productivity and effectiveness through information technology (IT).

- "Drudge" tasks that had previously consumed a lot of valuable human resource time are now partially or fully automated.
- Software programs are helping you expedite the processing of information and make better use of the information you have.
- Security planning and decision-making have benefited from "smart" programs that help you better understand countermeasures and trade-offs against the threat and that help you better control security costs.

*C*ertainly, we all want even more from the IT initiative and want it quicker. To do that, we need to share information on related work, successes, challenges, and the developing IT future. To help the community in that sharing, DoDSI will dedicate space for feedback on IT applications in security in our *Security Awareness Bulletin*, *Security Awareness News*, and special publications. We'll also expand our coverage of information technology in security in our training courses.

To do that well, we need you, our readers and students (government and contractor), to:

- Tell us about your specific uses of IT in your security programs; how well it's worked; the "agony and the ecstasy," the challenges and successes involved in getting it to work well; and the benefits and worries that go along with it.
- Show-off your electronic achievements to our faculty when they are in your area or you visit DoDSI.

*T*he key questions where you can help us and your fellow practitioners, are:

What Are We Really Doing?

If you've significantly bettered your security programs' application, costs/ benefits ratio, or use of human and other resources through information technology or have an ongoing project to do that, we want to hear about that so others can learn and benefit.

Initially, just send the information bulleted on the next page to DoDSI, ATTN: Carl Roper (IT Use), 8000 Jefferson Davis Highway, Richmond, VA 23297-5091. We'll contact you to discuss your application and, if agreed, work with you to publish information about it.

- Your name, position, organization, telephone number and mailing address.
- Brief description of your IT application, what it does and how long you have used it; or, if

under development, what's its intended use and when will you start to use it.

- Benefits you've received (or expect to receive) from the application in your security program and operation.
- How adaptable you think this application might be at other locations.

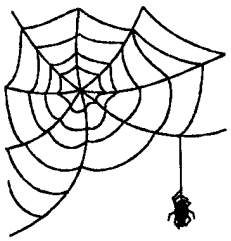
Note: Please exclude office software, such as word processing, desktop publishing, schedulers, visual presentation programs, graphics, graphing/charting, and spread sheet software unless you've made a unique use of them. Exclude generic applications, e.g., the EPSQ or commercial access control software, except when you've made a significant enhancement or improvement to them or how they are used. If in doubt, give us a call at 804 279-5593, or DSN 695-5593.

What Can You Show Us?

When our faculty is planning a trip in your neighborhood or you're coming to DoDSI, please let the faculty know if you've got an IT application you'd like to show-off. They'll arrange a visit to chat about it, see it, and help you in getting the word out to others that might benefit.

- Send us a brief on your IT application or on demonstrating your application
- Have your application selected as a feature article in a DoDSI publication

All we're really asking YOU to do is to brag a little about what you've done with information technology. Once you've done that, you can count on us to help you tell "the rest of the story." So, c'mon, electrify your community!



DoDSI is on the Web!

We're pleased to announce that the DoD Security Institute now has a home page on the Internet's World Wide Web. We're just getting started with the page, but we do have a few things available for you: course schedules and descriptions, some articles from past issues of the *Security Awareness Bulletin*, and a variety of other information. There's also a pretty substantial set of links to other pages with information you might find of interest. Our URL (address) is:

`http://www.dtic.mil/dodsi/`

When you visit the page, please take a couple of minutes to give us some feedback. The page will be growing, and we'd really appreciate hearing your comments and suggestions.

Seventh National Operations Security Conference

About the Conference

The conference, from April 15 through April 18, will focus on OPSEC applications throughout government and industry, with special focus on OPSEC in law enforcement, the private sector, and information warfare. Unclassified sessions, workshops, and seminars will be held at the McLean Hilton Hotel. Classified sessions will be held in the Hayes Building of Mitre Corporation. There will be no provision for security clearance certification at the conference. Certification must be provided to IOSS prior to the start of the conference.

Who Should Attend

Anyone involved in OPSEC, information warfare, or risk management, either as a manager, a policy-maker, or a practitioner will find interesting presentations and activities at the conference. There will be lots of sessions– some providing information, some provoking thought, and some providing training – for experts *and* beginners.

Exhibits

Equipment, programs, information, and training applications related to OPSEC will be on display at the National OPSEC Conference, Tuesday through Thursday. The newest information, tools, and training materials will be displayed and demonstrated by a wide variety of exhibitors. If you want to set up a booth, 8' x 10' spaces are still available. The cost is $900 for OPS members and $950 for nonmembers.

Registration

Fees

	Classified only	Conference only	Both
OPS Member	$50	$465	$515
Nonmember	$50	$490	$540

Accommodations

The McLean Hilton at Tysons Corner has been selected as the official headquarters for the National OPSEC Conference. Rooms have been reserved at $114 single/double and the prevailing government rate. To make reservations, please call 1-800-HILTONS or (703) 761-5111. Please mention the OPSEC Professionals Society when making your reservation to receive this special group rate. Reservations must be made by March 22, 1996.

Dulles and Washington National Airports are both conveniently located nearby. The McLean Hilton offers complimentary parking and provides complimentary van shuttle service between West Falls Church Metro and the hotel.

Name:_____ Nickname for Badge: _____

Organization:_____ Phone:_____ Fax:_____

Address:_____

Amount Enclosed: $_____ DD 1556 or SF 182 Enclosed_____

Payment may be made by check, money order, government training form, VISA or MasterCard. Checks and money orders should be made payable to OPSEC Professionals society. Those using training forms should ensure that payment is made promptly at conclusion of the conference.

Credit Card Payment: [ ] VISA [ ] MasterCard [ ] American Express

Card Number:_____ Expiration Date:_____

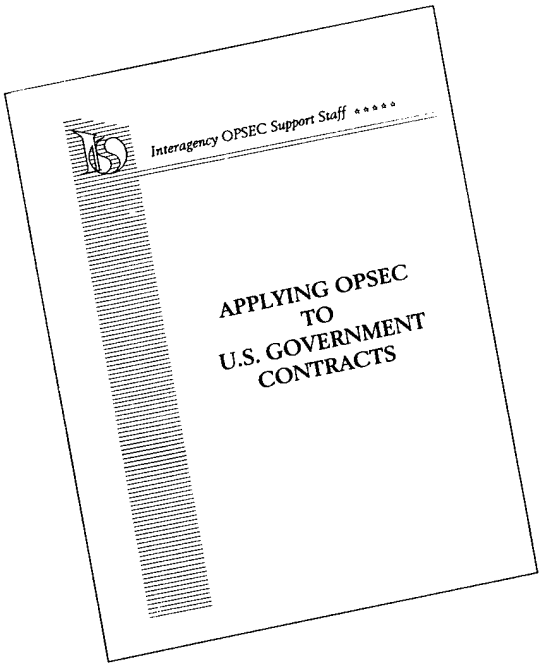
Name on Card:_____ Signature:_____

Please mail payment to: National OPSEC Conference
c/o WHA
P.O. Box 22606
Alexandria, VA 22304

Questions??? Call (703) 370-6329

Are you an OPSEC Certified professional?	Yes	No
Would you prefer to be excluded from the list of attendees?	Yes	No
Are you a first time attendee?	Yes	No
How would you like to receive your proceedings?	Disk	Hard Copy

Please note you will only receive your above selection on site. If you would like proceedings in both formats, there will be an additional charge to receive the other format.

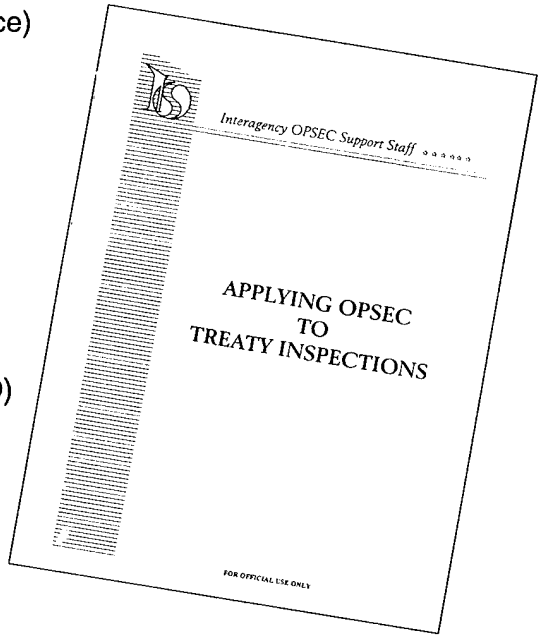


Interagency OPSEC Support Staff ☆ ☆ ☆ ☆ ☆

These publications may be ordered from :

Interagency OPSEC Support Staff (IOSS)
Attn: Ms. Mary L. Hodge
6411 Ivy Lane, Suite 400
Greenbelt, MD 20770-1405
Phone: (301) 982-5411; or form may be faxed to (301) 982-2913

- ❑ National Operations Security Doctrine (NOAC Issuance)
- ❑ The National OPSEC Program
- ❑ OPSEC Program Development Procedural Guide
- ❑ OPSEC Program Evaluation
- ❑ The Great Conversation: A History of OPSEC
- ❑ Compendium of OPSEC Terms
- ❑ Operations Security Planning — A Management Tool
- ❑ Brilliant Victory — The Channel Dash of 1942
- ❑ The Operations Security Void in the Drug War (FOUO)
- ❑ Applying OPSEC to Treaty Inspections (FOUO) (incorporates the eight previous Treaty publications)
- ❑ Applying OPSEC to U.S. Government Contracts



Please add my name to the IOSS mailing list ❑
I am currently on the IOSS mailing list ❑

Name (❑ Mr. ❑ Mrs. ❑ Ms.) (military rank): _____

Position/Title: _____

Organization: _____

Mailing address (business only): _____

_____

Phone (commercial only): ( ) _____

Contractors: Please provide the name of the Government agency sponsoring your major contract(s): _____

Interagency OPSEC Support Staff ☆ ☆ ☆ ☆ ☆

These videos may be ordered by returning this form to :

Interagency OPSEC Support Staff (IOSS)
Attn: Ms. Mary L. Hodge
6411 Ivy Lane, Suite 400
Greenbelt, MD 20770-1405
Phone: (301) 982-5411; or form may be faxed to (301) 982-2913

- ❑ OPSEC: Protecting Our Edge/OPSEC: Protecting Tomorrow's Technology Today (produced by DISA)
- ❑ OPSEC & Counternarcotics — Who's Watching Who? (produced by IOSS)
- ❑ Operations Security — An Overview (produced by Department of Energy); includes facilitator's guide
- ❑ The No-Tel Cartel: OPSEC in Action (produced by IOSS)
- ❑ The Missing Piece (produced by Lockheed)

Please add my name to the IOSS mailing list ❑
I am currently on the IOSS mailing list ❑

Name (❑ Mr. ❑ Mrs. ❑ Ms.) (military rank): _____

Position/Title: _____

Organization: _____

Mailing address (business only): _____

_____

Phone (commercial only): ( ) _____

Contractors: Please provide the name of the Government agency sponsoring your major contract(s): _____

Now available from the On-Site Inspection Agency:

ARMS CONTROL OUTREACH MATERIALS CATALOG

SPRING 1996

Readiness Through Awareness

Includes information on how to get bulletins, pamphlets, brochures, videos, and briefing support for your organization.

For copies call 1-800-419-2899 or write:

Attn: SECURITY OFFICER (SO)
ON-SITE INSPECTION AGENCY
201 WEST SERVICE ROAD, DULLES IAP
P.O. BOX 17498
WASHINGTON DC 20041-0498

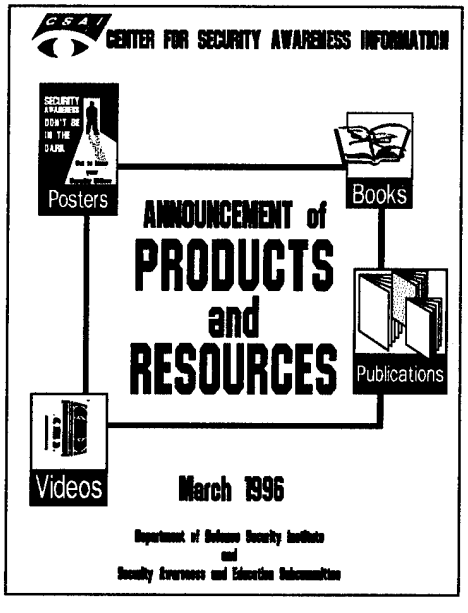
The first issue of the
Center for Security Awareness Information's

Announcement of Products and Resources

A catalog of information about new and time-tested videos, publications, computer-based educational products, briefing packages, and much more – tailored to meet the needs of the security educator in today's state-of-the-art training environment.

For several months CSAI staff has been busy cataloging new product submissions from government and industry, processing test audience data, and verifying source and ordering information. Our end product is the *Announcement* which provides product descriptions and ordering information and, for newer audiences, consumer feed-back based on test-audience reactions.

The products and publications cover a wide range of security concerns including information, personnel, industrial, and physical security, as well as the foreign intelligence and international terrorist threats.



The *Announcement of Products and Resources* will be helpful to the security educator in both industry and Federal government. Our plan is to update and re-issue the hard-copy publication every six months, but maintain a more continuously updated issue on the DoDSI Web site (see the DoDSI Web page ad also in this issue). The publication will reflect new information on products and resources provided by our readership in the government and contractor community.

Obtain your copy by using the ordering form for DoDSI publications on page 40 of this issue of the Bulletin. Or watch our Web-site for the appearance of this publication in electronic form.

The Center for Security Awareness Information is co-sponsored by the Department of Defense Security Institute and the Security Awareness and Education Subcommittee.

Security Awareness Publications Available from the Institute

Publications are free. Just check the titles you want and send this form to us with your **address label**

Our address is:

DoD Security Institute
Attn: SEAT
8000 Jefferson Davis Hwy, Bldg 33E
Richmond, VA 23297-5091
(804) 279-5314/4223 or DSN 695-5314/4223

- ❑ **Recent Espionage Cases: Summaries and Sources**. July 1994. Eighty-five cases, 1975 through 1994. "Thumb-nail" summaries and open-source citations.
- ❑ **Announcement of Products and Resources**. March 1996. A catalog of security education videos, publications, posters, and more you can order.
- ❑ **DELIVER!** Easy-to-follow pamphlet on how to transmit and transport your classified materials. Written specifically for the Department of Defense employee. September 1992.
- ❑ **Terminator VIII**. Requirements for destruction of classified materials. Written specifically for the Department of Defense employee. September 1992.
- ❑ **STU-III Handbook for Industry**. To assist FSOs of cleared defense contractors who require the STU-III, Type 1 unit. Covers step-by-step what you need to know and do to make the STU-III a valuable addition to your facility's operations.
- ❑ **Survival Handbook**. The basic security procedures necessary for keeping you out of trouble. Written specifically for the Department of Defense employee. April 1995.
- ❑ **Layman's Guide to Security**. The basic security procedures that you should be aware of when handling classified materials in your work environment. May 1995.
- ❑ **Acronyms and Abbreviations**. Twelve pages of security-related acronyms and abbreviations and basic security forms. October 1995.
- ❑ **Take A Security Break.** Questions and answers on security and other topics.
- ❑ **Take Another Security Break.** More questions and answers.
- ❑ **Lock Up!** A pamphlet on the structural standards and other security requirements for the storage of conventional arms, ammunition, and explosives. August 1995.

Security Awareness Bulletin. A quarterly publication of current security countermeasures and counterintelligence developments, training aids, and education articles. Back issues available from the Institute:

- ❑ The Case of Randy Miles Jeffries **(2-90)**
- ❑ Beyond Compliance - Achieving Excellence in Industrial Security **(3-90)**
- ❑ Foreign Intelligence Threat for the 1990s **(4-90)**
- ❑ Regional Cooperation for Security Education **(1-91)**
- ❑ AIS Security **(2-91)**
- ❑ Economic Espionage **(1-92)**
- ❑ OPSEC **(3-92)**
- ❑ What is the Threat and the New Strategy? **(4-92)**
- ❑ Acquisition Systems Protection **(1-93)**
- ❑ Treaty Inspections and Security **(2-93)**
- ❑ Research on Espionage **(1-94)**
- ❑ Information Systems Security **(2-94)**
- ❑ Acquisition Systems Protection Program **(3-94)**
- ❑ Aldrich H. Ames Espionage Case **(4-94)**
- ❑ Revised Self-Inspection Handbook/Summary of NISPOM Changes **(1-95)**
- ❑ The Threat to U.S. Technology **(2-95)**
- ❑ Entering a New Era in Security **(1-96)**

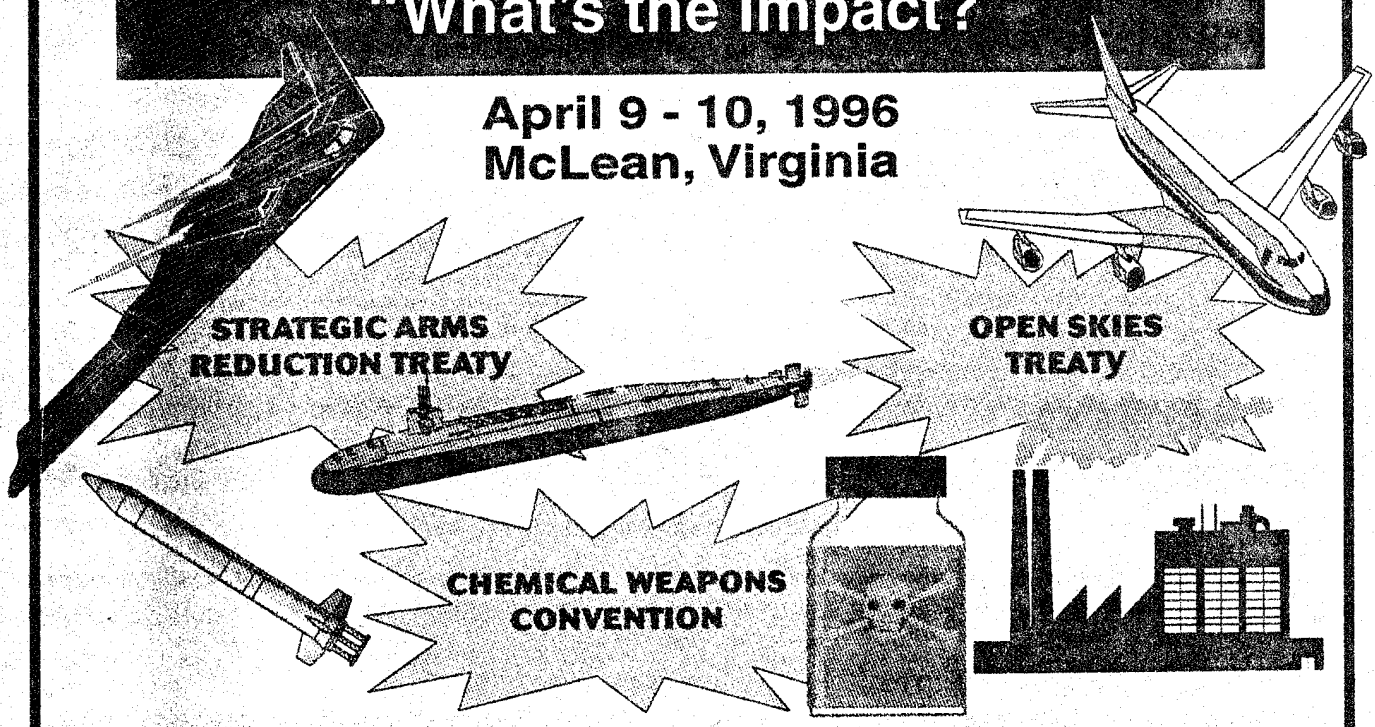
*U.S. Government Printing Office: 1996 - 728-109/40003

DTIRP

DEFENSE TREATY INSPECTION READINESS PROGRAM

Arms Control Seminar for Industry
"What's the Impact?"

April 9 - 10, 1996
McLean, Virginia



Prior Attendees Include:

Aegis Research Corp
Aerojet Corp
Anser Corp
Atlantic Research Corp
Autometric Inc
Babcock & Wilcox Corp
Beta Analytics Inc
Boeing Corp
Computer Sciences Corp
CTA Space Systems
Dyncorp
E-Systems Inc
GTE Government Systems
Harris Corp
Honeywell Inc
Hughes Aircraft Co
Lawrence Livermore Labs
Lockheed Sanders Inc
Loral Vought Systems Corp
Martin Marietta Corp
McDonnel-Douglas Corp
Northrop Grumman Corp
Olin Ordnance
Raytheon Co
Rockwell International Corp
SAIC
SRI International
Titan Systems Group
Trident Data Systems
Unisys Corp
Veda Corp
3M Company

For More Information Call: 1-800-419-2899